Chapter 2 Procedures

FUNCTION OVERVIEW 2-2

1 SYSTEM SECURITY 2-3
1.1 Add STAB Table 2-3
1.2 Change STAB Table 2-6
1.3 Delete STAB Table 2-8
1.4 Inquire STAB Table 2-10

2 SCREEN SECURITY 2-11
2.1 Add FORT Table 2-11
2.2 Change FORT Table 2-14
2.3 Delete FORT Table 2-16
2.4 Inquire FORT Table 2-18

3 RECORD SECURITY 2-19
3.1 Add Access Authority Table 2-19
3.2 Change Access Authority Table 2-20
3.3 Delete Access Authority Table 2-21
3.4 Inquire Access Authority Table 2-22

4 DATA ELEMENT SECURITY 2-23
4.1 Add Data Element Security 2-23
4.2 Change Data Element Security 2-24
4.3 Delete Data Element Security 2-25
4.4 Inquire Data Element Security 2-26

Function Overview

The purpose of this chapter is to describe the procedures required to establish and maintain AGPS Security.

1 SYSTEM SECURITY

1.1 Add STAB Table

Overview

System security in AGPS is controlled by USERID and Security Group. This is accomplished with use of STAB screen. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required security group

Outputs

- **!** Updated STAB Table record

Completing The Procedure

Cross-Reference Steps

1. Determine system access requirements. This may be accomplished by the following method(s).

   a. You may perform a survey of all agencies or a specific agency to determine user system access requirements.

   b. You may, instead of a survey, wait until an agency identifies a user system access requirement to update the STAB Table.

2. Add STAB Table data into AGPS.

   The STAB (Security) table is used to do two things. First is to link persons to security groups. Second is to restrict or allow functions normally performed by the screens in the security group.

   This is accomplished by assigning the established security groups to USERIDs and allowing/restricting normal program functions. Each USERID and password may be assigned a maximum of 9 security groups. The functions (add, change, delete and inquiry) may be different for each group or they can be the same.

   a. If the user is not in the STAB screen, type **STAB** in the Function Line and press RETURN/ENTER.

3. Type **A** in the Action Line.

a. Using the TAB key, move to USERID field and type the desired USERID.

b. Using the TAB key, move to Security Group field and type the desired security group.

The group(s) identification (BUYR, INQR, etc.) to be assigned that USERID and password.

c. Using the TAB key, move to SCAN ACT field and type desired indicator. Must be Y or N. Set to Y for INQUIRE function.

d. Using the TAB key, move to APPROVAL ACT field and type desired indicator. Always set to N. This field has nothing to do with the security. This is a CORE approval. AGPS has its own approvals process.

e. Using TAB key, move to ENTER ACT field and type desired indicator. Must be Y or N. Set to Y for add, change or delete. If correct act, delete act or sched act is set to Y then this field must be Y.

f. Using TAB key, move to CORRECT ACT field and type desired indicator. Must be Y or N. Set to Y for CHANGE function.

g. Using TAB key, move to DELETE ACT field and type desired indicator. Must be Y or N. Set to Y for DELETE function.

h. Using TAB key, move to SCHED ACT field and type desired indicator. Must be Y or N. Set to Y for ADD function.

i. Using Tab key, move to EDIT ONLY ACT field and type desired indicator. Must be Y or N. Set to Y for INQUIRE function. If scan act is Y then this field must be Y.

j. The remaining fields on the STAB table are not applicable to the security aspects of AGPS. However they have specific values which will be assigned and not changed.

NOTE: On at least one USERID (System Administrator), the security group on the STAB must have an *ALL so that person can have access to all screens. This acts as a wild card and without it, access to the system could be denied.

The following is an example of assigning the BUYR, ENTR and INQR groups to USERID and password BARNSULL using the STAB table. Remember the groups have already been assigned to the screen using the FORT table.

```
          USERID:  BARNSULL

                        1     2     3     4     5     ETC.

   SECURITY GROUP:   BUYR  ENTR  INQR
         SCAN ACT:   Y     Y     Y
      APPROVAL ACT:  N     N     N
         ENTER ACT:  Y     Y     N
       CORRECT ACT:  Y     Y     N
        DELETE ACT:  Y     Y     N
         SCHED ACT:  Y     Y     N
     EDIT ONLY ACT:  Y     Y     Y
          HOLD ACT:  N     N     N
           RUN ACT:  N     N     N
RUN IMMEDIATE ACT:   N     N     N
FORWHOM TEST TYPE:   0     0     0
  WHERE TEST TYPE:   0     0     0
       WHERE CODE:   0     0     0
         OVERRIDE:   1     1     1
        APPROVALS:   NNNNN NNNNN NNNNN
```

NOTE: Prior to the system becoming operational, the security needs to go in the screen gen to prevent it from getting lost. If this is not done then each time a screen is generated, the security will be lost.

4. Press RETURN/ENTER.

NOTE: If an error condition exists, AGPS will display the appropriate error messages at the bottom of the transaction screen. Clear the error conditions identified and press RETURN/ENTER. If no error(s) exists, AGPS will display 'UPDATE SCREEN PROCESSED'.

1.2 Change STAB Table

Overview

System security in AGPS is maintainable by USERID. This is accomplished with use of STAB screen. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required changes to security group

Outputs

- **!** Updated STAB Table record

Completing The Procedure

Cross-Reference Steps

1. Determine system access change requirements. This may be accomplished by the following method(s).
   a. You may perform a survey of all agencies or a specific agency to determine user system access change requirements.
   b. You may, instead of a survey, wait until an agency identifies a user system access change requirement to update the STAB Table.
2. Change STAB Table data in AGPS.
   a. If the user is not in the STAB screen, type **STAB** in the Function Line and press RETURN/ENTER.
3. Type **S** in the Action Line.
   a. Using the TAB key, move to USERID field and type the desired USERID.
   b. Press RETURN/ENTER. Requested STAB record should be displayed.
4. Type **C** in the Action Line.
   a. Using the TAB key, move to Security Group field and type the desired security group.

The group(s) identification (BUYR, INQR, etc.) to be assigned that USERID and password.

b. Using the TAB key, move to SCAN ACT field and type desired indicator. Must be Y or N. Set to Y for INQUIRE function.

c Using the TAB key, move to APPROVAL ACT field and type desired indicator. Always set to N. This field has nothing to do with the security. This is a CORE approval. AGPS has its own approvals process.

d. Using TAB key, move to ENTER ACT field and type desired indicator. Must be Y or N. Set to Y for add, change or delete. If correct act, delete act or sched act is set to Y then this field must be Y.

e. Using TAB key, move to CORRECT ACT field and type desired indicator. Must be Y or N. Set to Y for CHANGE function.

f. Using TAB key, move to DELETE ACT field and type desired indicator. Must be Y or N. Set to Y for DELETE function.

g. Using TAB key, move to SCHED ACT field and type desired indicator. Must be Y or N. Set to Y for ADD function.

h. Using TAB key, move to EDIT ONLY ACT field and type desired indicator. Must be Y or N. Set to Y for INQUIRE function. If scan act is Y then this field must be Y.

i. The remaining fields on the STAB table are not applicable to the security aspects of AGPS. However they have specific values which will be assigned and not changed.

5. Press RETURN/ENTER.

NOTE: If an error condition exists, AGPS will display the appropriate error messages at the bottom of the transaction screen. Clear the error conditions identified and press RETURN/ENTER. If no error(s) exists, AGPS will display 'ALL LINES CHANGED'.

1.3 Delete STAB Table

Overview

System security in AGPS may be deleted by USERID and Security Group. This is accomplished with use of STAB screen. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required security group

Outputs

- **!** Updated STAB Table record

Completing The Procedure

Cross-Reference Steps

1. Determine system access delete requirements. This may be accomplished by the following method(s).
   a. You may perform a survey of all agencies or a specific agency to determine user system access delete requirements.
   b. You may, instead of a survey, wait until an agency identifies a user system access delete requirement to update the STAB Table.
2. Delete STAB Table data in AGPS.
   a. If the user is not in the STAB screen, type **STAB** in the Function Line and press RETURN/ENTER.
3. Type **S** in the Action Line.
   a. Using the TAB key, move to USERID field and type the desired USERID.
   b. Press RETURN/ENTER. Requested STAB record should be displayed.
4. Type **D** in the Action Line. If entire record is to be deleted, proceed to step 5.
   a. Using the TAB key, move to Security Group field and space out the desired security group. If security group is not spaced, it will be deleted.

5. Press RETURN/ENTER.

NOTE: If an error condition exists, AGPS will display the appropriate error messages at the bottom of the transaction screen. Clear the error conditions identified and press RETURN/ENTER. If no error(s) exists, AGPS will display 'ALL LINES DELETED'.

1.4 Inquire STAB Table

Overview

System security in AGPS may be inquired by USERID. This is accomplished with use of STAB screen. Access is limited to the System Administrator.

Inputs

! Required userid

Outputs

! Display of requested STAB Table record

Completing The Procedure

Cross-Reference Steps

1. Determine system access to be inquired.
2. Inquire STAB Table data in AGPS.
   a. If the user is not in the STAB screen, type **STAB** in the Function Line and press RETURN/ENTER.
3. Type **S** in the Action Line.
   a. Using the TAB key, move to USERID field and type the desired USERID.
4. Press RETURN/ENTER.

   NOTE: If an error condition exists, AGPS will display the appropriate error messages at the bottom of the transaction screen. Clear the error conditions identified and press RETURN/ENTER. If no error(s) exists, AGPS will display requested STAB Table record.

2 SCREEN SECURITY

2.1 Add FORT Table

Overview

Screen security in AGPS is controlled by Security Group. This is accomplished with use of FORT screen. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required screen identifier
- **!** Required security group

Outputs

- **!** Updated FORT Table record

Completing The Procedure

Cross-Reference Steps

1. Determine screen access requirements. This may be accomplished by the following method(s).

   a. You may perform a survey of all agencies or a specific agency to determine user screen access requirements.

   b. You may, instead of a survey, wait until an agency identifies a user screen access requirement to update the FORT Table.

   Before setting up security, Purchasing must logically analyze the kind of security that will be required for screens, records and data elements. This is done by analyzing the functions to be performed and logically associating persons to those groups. That is, common functions should be associated with screens and the persons performing those functions should be given access to those screens. These groups then become security groups. These security groups should cross organizational lines so long as the functions being performed are common within the group.

   Examples of typical groups are:

   1). BUYR: Used by all buyers and buyer assistants for requisitions, solicitations, orders and contracts.

2). ENTR: Used for data entry of all document types using screens such as RQS4, RLI2, RACG, ORD4, OLI3, OACG, etc.

3). BIDL: Used for bid list management, vendor records maintenance and vendor commodity registration.

4). COMD: Used by commodity maintenance personnel for maintaining commodity items and commodity specifications.

5). INQR: Assigned to all screens to provide inquiry capability.

A security group should cover several screens or all the screens that group of persons should have access to.

2. Add FORT Table data into AGPS.

The FORT (Format) table is used to establish the security groups for a screen. In the FORT table each screen may be assigned to a maximum of 4 security groups. From a security point of view, the FORT table assigns a screen to security group(s).

The security groups assigned to a screen on the FORT table should be organized in least restrictive to most restrictive order, left to right. A group with a screen allowing add, change, delete would be least restrictive. A group with a screen allowing inquiry only would be most restrictive.

FORT table examples could be:

a. SDOC could have security groups BUYR, ENTR and INQR.

b. RQS4 could have security groups ENTR and INQR.

c. If the user is not in the FORT screen, type **FORT** in the Function Line and press RETURN/ENTER.

3. Type **S** in the Action Line.

a. Using the TAB key, move to Format Def Key field and type the desired screen identifier.

b. Press RETURN/ENTER. Requested FORT Table screen record should be displayed.

4. Type **C** in the Action Line.

a. Using the TAB key, move to the Security Group field(s) and type desired security group.

5. Press RETURN/ENTER.

NOTE: If an error condition exists, AGPS will display the appropriate error messages at the bottom of the transaction screen. Clear the error conditions identified and press RETURN/ENTER. If no error(s) exists, AGPS will display 'ALL LINES CHANGED'.

Whether a screen can perform a function is obviously controlled by the program behind the screen. If the program is not coded to perform a function, then the function cannot be performed. However, if the program is coded to perform a function, the function can be allowed for certain USERIDs and restricted for other USERIDs.

2.2 Change FORT Table

Overview

Screen security in AGPS may be changed by Security Group. This is accomplished with use of FORT screen. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required screen identifier
- **!** Required security group

Outputs

- **!** Updated FORT Table record

Completing The Procedure

Cross-Reference Steps

1. Determine screen access change requirements. This may be accomplished by the following method(s).
   a. You may perform a survey of all agencies or a specific agency to determine user screen access change requirements.
   b. You may, instead of a survey, wait until an agency identifies a user screen access change requirement to update the FORT Table.
2. Change FORT Table data in AGPS.
   a. If the user is not in the FORT screen, type **FORT** in the Function Line and press RETURN/ENTER.
3. Type **S** in the Action Line.
   a. Using the TAB key, move to Format Def Key field and type the desired screen identifier.
   b. Press RETURN/ENTER. Requested FORT Table screen record should be displayed.
4. Type **C** in the Action Line.
   a. Using the TAB key, move to the Security Group field(s) and type desired security group.

5. Press RETURN/ENTER.

NOTE: If an error condition exists, AGPS will display the appropriate error messages at the bottom of the transaction screen. Clear the error conditions identified and press RETURN/ENTER. If no error(s) exists, AGPS will display 'ALL LINES CHANGED'.

2.3 Delete FORT Table

Overview

Screen security in AGPS may be deleted by Security Group. This is accomplished with use of FORT screen. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required screen identifier
- **!** Required security group

Outputs

- **!** Updated FORT Table record

Completing The Procedure

Cross-Reference Steps

1. Determine screen access security group to be deleted.
2. Delete FORT Table security group data in AGPS.
   a. If the user is not in the FORT screen, type **FORT** in the Function Line and press RETURN/ENTER.
3. Type **S** in the Action Line.
   a. Using the TAB key, move to Format Def Key field and type the desired screen identifier.
   b. Press RETURN/ENTER. Requested FORT Table screen record should be displayed.
4. Type **D** in the Action Line.
   a. Using the TAB key, move to the Security Group field(s) and space out desired security group. If not spaced out, security group will be deleted. **NEVER PERFORM DELETE ON FORT TABLE RECORD WITH ALL SECURITY GROUPS EQUAL SPACES. THIS WILL RESULT IN ACCESS TO SCREEN BEING DENIED TO ALL USERS.**
5. Press RETURN/ENTER.

NOTE: If an error condition exists, AGPS will display the appropriate error messages at the bottom of the transaction screen. Clear the error conditions identified and press RETURN/ENTER. If no error(s) exists, AGPS will display 'ALL LINES DELETED'.

2.4 Inquire FORT Table

Overview

Screen security in AGPS may be inquired by Screen Identifier. This is accomplished with use of FORT screen. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required screen identifier

Outputs

- **!** Updated FORT Table record

Completing The Procedure

Cross-Reference Steps

1. Determine screen access to be inquired.
2. Delete FORT Table security group data in AGPS.
   a. If the user is not in the FORT screen, type **FORT** in the Function Line and press RETURN/ENTER.
3. Type **S** in the Action Line.
   a. Using the TAB key, move to Format Def Key field and type the desired screen identifier.
   b. Press RETURN/ENTER. Requested FORT Table screen record should be displayed.
4. Press RETURN/ENTER.

   NOTE: If an error condition exists, AGPS will display the appropriate error messages at the bottom of the transaction screen. Clear the error conditions identified and press RETURN/ENTER. If no error(s) exists, AGPS will display requested FORT Table record.

3 RECORD SECURITY

3.1 Add Access Authority Table

Overview

Record security in AGPS is established by use of the BAAT Table. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required agency number
- **!** Required maintenance indicator

Outputs

- **!** Updated BAAT Table record

Completing The Procedure

Cross-Reference	Steps
	1. See Section 1, Installation Tables Maintenance, Chapter 2, Paragraph 1, Add/Change Access Authority Table, Subparagraph 1.1, Add Access Authority Table.

3.2 Change Access Authority Table

Overview

Record security in AGPS is maintained by use of the BAAT Table. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required change to agency number
- **!** Required change to maintenance indicator

Outputs

- **!** Updated BAAT Table record

Completing The Procedure

Cross-Reference Steps

1. See Section 1, Installation Tables Maintenance, Chapter 2, Paragraph 1, Add/Change Access Authority Table, Subparagraph 1.3, Change Access Authority Table.

3.3 Delete Access Authority Table

Overview

Record security in AGPS may be deleted by use of the BAAT Table. Access is limited to the System Administrator.

Inputs

! Required userid

Outputs

! Updated BAAT Table record

Completing The Procedure

Cross-Reference	Steps
	1. See Section 1, Installation Tables Maintenance, Chapter 2, Paragraph 1, Add/Change Access Authority Table, Subparagraph 1.4, Delete Access Authority Table.

3.4 Inquire Access Authority Table

Overview Record security in AGPS may be inquired by use of the BAAT Table. Access is limited to the System Administrator.

Inputs
- **!** Required userid

Outputs
- **!** Display of requested BAAT Table record

Completing The Procedure

Cross-Reference	Steps
	1. See Section 1, Installation Tables Maintenance, Chapter 2, Paragraph 1, Add/Change Access Authority Table, Subparagraph 1.5, Inquire Access Authority Table.

4 DATA ELEMENT SECURITY

4.1 Add Data Element Security

Overview Data element security in AGPS is established by use of the BAAT Table. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required authorization code

Outputs

- **!** Updated BAAT Table record

Completing The Procedure

Cross-Reference	Steps
	1. See Section 1, Installation Tables Maintenance, Chapter 2, Paragraph 1, Add/Change Access Authority Table, Subparagraph 1.2 Establish Screen Processing Authorization.

4.2 Change Data Element Security

Overview

Data element security in AGPS is maintained by use of the BAAT Table. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required change to authorization code

Outputs

- **!** Updated BAAT Table record

Completing The Procedure

Cross-Reference	Steps
	1. See Section 1, Installation Tables Maintenance, Chapter 2, Paragraph 1, Add/Change Access Authority Table, Subparagraph 1.3 Change Access Authority Table.

4.3 Delete Data Element Security

Overview

Data element security in AGPS may be deleted by use of the BAAT Table. Access is limited to the System Administrator.

Inputs

- **!** Required userid
- **!** Required authorization code

Outputs

- **!** Updated BAAT Table record

Completing The Procedure

Cross-Reference	Steps
	1. See Section 1, Installation Tables Maintenance, Chapter 2, Paragraph 1, Add/Change Access Authority Table, Subparagraph 1.4 Delete Access Authority Table.

4.4 Inquire Data Element Security

Overview

Data element security in AGPS may be inquired by use of the BAAT Table. Access is limited to the System Administrator.

Inputs

! Required userid

Outputs

! Display of requested BAAT Table record

Completing The Procedure

Cross-Reference	Steps
	1. See Section 1, Installation Tables Maintenance, Chapter 2, Paragraph 1, Add/Change Access Authority Table, Subparagraph 1.5 Inquire Access Authority Table.